REMARKS

The present application was filed on June 20, 2003 with claims 1-16. Claims 1, 8, 9 and 16 are the independent claims.

In the outstanding Office Action, the Examiner: (i) rejected claims 1, 2, 4-6, 8-10, 12-14 and 16 under 35 U.S.C.§103(a) as being unpatentable over U.S. Patent No. 6,697,488 (hereinafter "Cramer") in view of U.S. Patent No. 5, 515, 441 (hereinafter "Faucher"); and (ii) rejected claims 3, 7, 11 and 15 under 35 U.S.C.§103(a) as being unpatentable over Cramer and Faucher in view of a Cramer et al. article entitled "Multiparty Computation from Threshold Homomorphic Encryption" (hereinafter "Cramer paper").

In this response, Applicant amends independent claims 1, 8, 9 and 16 and respectfully requests reconsideration of the present application in view of the remarks below.

Currently amended claim 1 is directed to a method for use in a device associated with a first party for decrypting a ciphertext according to a Cramer-Shoup based encryption scheme, the method comprising the steps of: obtaining the ciphertext in the first party device sent from a device associated with a second party; and generating in the first party device a plaintext corresponding to the ciphertext based on assistance from the second party device, wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device, the plaintext representing a result of the decryption according to the Cramer-Shoup based encryption scheme, such that the first party device and the second party device jointly decrypt the ciphertext but neither can decrypt the ciphertext alone. The last phrase (underlined) is being added by the present amendment. Support for the amendment can be found throughout the present specification, for example, see page 4, lines 13-17. Independent claims 8, 9 and 16 have been amended in a similar manner.

With regard to the §103(a) rejections, Applicant initially notes that a proper case of obviousness requires that the cited references when combined must "teach or suggest all the claim limitations," and that there be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine the references or

to modify the reference teachings. See Manual of Patent Examining Procedure (MPEP), Eighth Edition, August 2001, §706.02(j).

Applicant submits that the Examiner has failed to establish a proper case of obviousness in the §103(a) rejection of claims 1, 2, 4-6, 8-10, 12-14 and 16 over Cramer and Faucher, in that the Cramer and Faucher references, even if assumed to be combinable, fail to teach or suggest all the claim limitations, and in that no cogent motivation has been identified for combining the references or modifying the reference teachings to reach the claimed invention.

The present invention provides an efficient and provably secure protocol by which two parties, respectively designated herein as "alice" (or a first party) and "bob" (or a second party), each holding a share of a Cramer-Shoup private key, can jointly decrypt a ciphertext, but such that neither alice nor bob can decrypt a ciphertext alone. By way of one example, the invention can be used for a secure distributed third-party decryption service, which requires the joint agreement by two parties to decrypt a ciphertext. For example, this may be used to provide added security to: (1) a key recovery system by law enforcement, or (2) an "offline trusted third party" system in a fair exchange protocol. Another application involves techniques by which a device that performs private key operations (signatures or decryptions) in networked applications, and whose local private key is activated with a password or PIN (personal identification number), can be immunized against offline dictionary attacks in case the device is captured. Briefly, the goal of immunization against offline attack may be achieved by involving a remote server in the device's private key computations, essentially sharing the cryptographic computation between the device and the server.

Alice and bob obtain public and secret data through a trusted initialization procedure. After initialization, communication between alice and bob occurs in sessions (or decryption protocol runs), one per ciphertext that they decrypt together. Alice plays the role of session initiator in the decryption protocol. That is, alice receives requests to decrypt ciphertexts, and communicates with bob to decrypt these ciphertexts. We presume that each message between alice and bob is implicitly labeled with an identifier for the session to which it belongs. Multiple decryption sessions may be executed concurrently.

Each and every limitation of the independent claims is not met by the collective teachings of Cramer and Faucher. Below, Applicant explains how such portions of Cramer and Faucher fail to teach or suggest each and every limitation. While Applicant may refer from time to time to each reference alone in describing its deficiencies, it is to be understood that such arguments are intended to point out the overall deficiency of the cited combination.

Although Cramer at column 8, lines 25-35 refers to two devices, a sending device and a receiving device, and section V (column 9) of Cramer refers to a decryption scheme, Cramer does not meet certain limitations of amended claim 1 as alleged. For example, Cramer does not disclose assistance from one device with respect to the other device that comprises an exchange of information between the devices such that the first party device and the second party device jointly decrypt the ciphertext but neither can decrypt the ciphertext alone, as now recited in the claimed invention. The devices in Cramer are not jointly decrypting the ciphertext, and Cramer does not impose the limitation that neither party can decrypt the ciphertext alone.

The Faucher reference fails to remedy the above-noted deficiencies of Cramer as applied to claim 1. Accordingly, it is believed that the combined teachings of Cramer and Faucher fail to meet the limitations of claim 1.

Also, the Examiner has failed to identify a cogent motivation for combining Cramer and Faucher in the manner proposed. The Examiner provides the following statement of motivation beginning at page 7, third paragraph of the Office Action:

> Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Faucher's reference within Cramer to include wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device. One of ordinary skill in the art would have been motivated to do this because it would secure communications conducted over insecure channels using public-keys method (col. 1, lines 13-15).

In response to Applicant's arguments, the Examiner provides the following statement of motivation on page 3 of the Office Action:

> Furthermore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Faucher's reference within Cramer to include wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device. One of ordinary skill in the art would have been motivated to do this because it would secure communications conducted over insecure channels using public-key methods (Faucher, col. 1, lines 13-15.

Applicant respectfully submits that these are conclusory statements of the sort rejected by both the Federal Circuit and the U.S. Supreme Court. See KSR v. Teleflex, No. 13-1450, slip. op. at 14 (U.S., Apr. 30, 2007), quoting In re Kahn, 441 F. 3d 977, 988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."). There has been no showing in the present §103(a) rejection of claim 1 of objective evidence of record that would motivate one skilled in the art to combine Cramer and Faucher to produce the particular limitations in question. The above-quoted statement of motivation provided by the Examiner appears to be a conclusory statement of the type ruled insufficient in KSR v. Teleflex.

For at least these reasons, Applicant asserts that claim 1 is patentable over Cramer and Faucher.

Currently amended independent claim 9 includes limitations similar to those of claim 1, and is therefore believed allowable for reasons similar to those described above with reference to claim 1.

Currently amended claims 8 and 16, which recite limitations from the perspective of the device providing assistance to the decrypting device, and include limitations similar to those of claim 1, are therefore believed allowable for reasons similar to those described above with reference to claim 1. For at least these reasons, Applicant asserts that claims 8 and 16 are patentable over Cramer and Faucher.

Dependent claims 2, 4-6, 10 and 12-14 are allowable for at least the reasons identified above with regard to claims 1 and 9. One or more of these claims are also believed to define separately-patentable subject matter over the cited art.

Claims 2 and 10 recite an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party can not read the information but can use the information to perform an operation. The Examiner refers to Cramer at column 7, lines 1-40 and column 9, lines 25-45 as teaching or suggesting the limitations of claims 2 and 10. Although Cramer at column 7, lines 25-26 refers to a public key represented by the numbers $g_1$, $g_2$, c, d, and h, the relied-upon portions of Cramer do not teach or suggest an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party cannot read the information but can use the information to perform an operation.

Claims 4 and 12 recite generating a share of a random secret; generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext; transmitting at least the encrypted information to the second party device; and computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device. The Examiner refers to Cramer at column 7, lines 11-19 as teaching or suggesting the step of generating a share of a random secret. The relied-upon portion of Cramer refers to a private-key choosing step, and does not teach or suggest generating a share of a random secret. Although Cramer, at column 7, lines 10-27 refers to private key $Z_q$, the relied-upon portions of Cramer do not teach or suggest generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext. Furthermore, although Cramer at column 9, lines 25-50 refers to recovering the plaintext m in the decryption step 50, Cramer does not teach or suggest computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device.

With regard to claims 5 and 13, the relied-upon portions of Cramer do not teach or suggest the recited limitation. Column 7, lines 10-15 of Cramer refers to private-key choosing step 13, and column 9, lines 35-40 refer to decryption of an encryption of a message, which do not teach or suggest the first party device and the second party device additively share components of a private key.

With regard to claims 6 and 14, Cramer at column 8, line 38 through column 9, line 23 refers to verification of ciphertext 30 in verification step 40. Although the relied-upon portion of Cramer refers to verifying ciphertext 30, the relied-upon portion of Cramer does not teach or suggest generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party.

Accordingly, withdrawal of the §103(a) rejection of claims 1, 2, 4-6, 8-10 12-14 and 16 is respectfully requested.

With regard to the rejection of claims 3, 7, 11 and 15 as being unpatentable over Cramer and Faucher in view of Cramer paper, Applicant asserts that the Cramer paper reference fails to remedy the deficiencies described above with regard to Cramer and Faucher. Thus, claims 3, 7, 11 and 15 are patentable at least by virtue of their dependency from claims 1 and 9. Claims 3, 7, 11 and 15 also recite patentable subject matter in their own right.

Accordingly, withdrawal of the §103(a) rejection of claims 3, 7, 11 and 15 is respectfully requested.

In view of the above, Applicant believes that claims 1-16 are in condition for allowance, and respectfully requests withdrawal of the various §103(a) rejections.

Respectfully submitted,



Date: February 29, 2008

William E. Lewis
Attorney for Applicant(s)
Reg. No. 39,274
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946